(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－282673

(43)公開日　平成11年(1999)10月15日

(51)Int.Cl.[6]		識別記号	FI		
G06F	9/06	550	G06F	9/06	550Z
	11/34			11/34	C
	12/14	310		12/14	310F

審査請求　未請求　請求項の数9　FD　（全 10 頁）

(21)出願番号　特願平10－101933

(22)出願日　平成10年(1998)３月31日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　櫻　修
東京都府中市東芝町１番地　株式会社東芝府中工場内

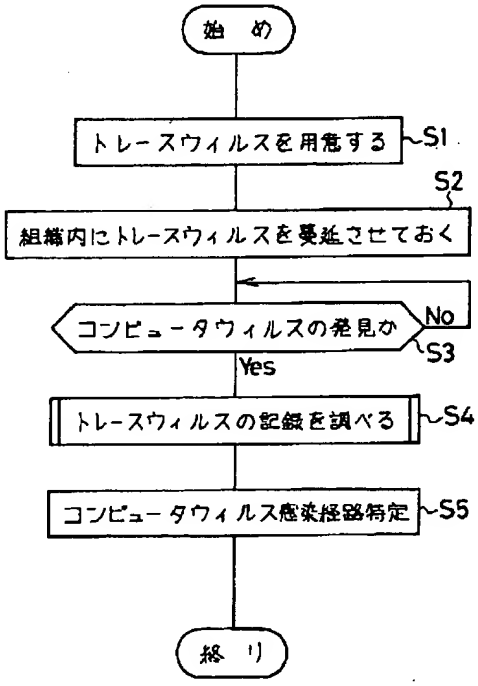
(74)代理人　弁理士　紋田　誠

(54)【発明の名称】　コンピュータウィルスの感染経路検出方法とその方法に用いるトレースウィルスを記録する記録媒体

(57)【要約】

【課題】　感染の経路を早期に検出して未然防止と感染を根絶する。

【解決手段】　コンピュータウィルスと同様の自己複製機能を有し、コンピュータウィルスと同様の感染経路をとると想定される感染履歴を記録するコンピュータウィルスと無関係のトレースウィルスを特定の調査領域内に蔓延させ、コンピュータウィルスが発見されたとき、発見された文書等に存在するトレースウィルスを起点にして特定の調査領域内のトレースウィルスの感染履歴を順次調べて、感染履歴に基づいてトレースウィルスの感染ルートを探索して特定し、特定されたトレースウィルスの感染ルートに基づいてコンピュータウィルス感染ルートを推定して特定の調査領域への侵入箇所を検出する。



発病するための特定時刻、一定時間、処理時間等の条件を記憶させて、発病するまで症状を出さない。
（3）　発病
プログラムやデータなどのファイルの破壊を行ったり、設計者の意図しない動作をする。以上の（1）～（3）の出典は情報処理振興事業協会（IPA）によるものである。
【0004】コンピュータウィルスの種類
（1）　機械語ウィルス
a）　システム感染型（ブートセクタ型）
HDD中のIPL（ブートセクタ、パーティションテーブル）に感染し、起動後には既に感染状態になっている。
b）　ファイル感染型（アプリケーション感染型）
感染したプログラム／データを実行すると、他のプログラム／データに感染する場合と、実行の際に日付や実行回数などの条件が満足されていると発病する場合がある。
（2）　マクロウィルス
文書ファイル（例、Word、Excel）に感染するタイプで、同一マクロ体系の機種やOSの違いを越えるマルチプラツトホーム型である。文書ファイルオープン時に他の同一ファイル形式のマクロに感染する。
【0005】コンピュータウィルスの感染経路には以下の様なケースが考えられる。
1）FDやCD－ROM配布により感染
2）パソコン通信、WWWサーバ、ファイルサーバ等からダウンロードしたプログラムやデータから感染
3）電子メールやグループウェア等の添付ファイルから感染
【0006】特に、最近は、ネットワーク環境の広まりにより、上記（2）（3）のケースによる被害がクローズアップされている。その一方、ウィルスチェックソフトやワクチンソフトの進歩も著しく、相応の準備さえ行っていれば、ウィルス感染の早期発見、被害拡大の防止はかなりの程度行うことができるようになってきている。
【0007】
【発明が解決しようとする課題】しかし、現在の技術では、ウィルスチェックソフトによるウィルス感染の発見後、又は、不幸にして発病による感染の発覚後に、それ以上の被害拡大を防ぐ処置はできても、そのウィルスがどの様な経路で感染してきたかの特定が困難なため、感染源を追求し、再感染の防止や根絶を行うことができないという問題がある。
【0008】そこで、本発明の目的は、従来技術の持つこのような問題点の解決、すなわち、コンピュータウィルスが発見されたときに、そのウィルスがどういう経路で感染してきたかを明らかにするコンピュータウィルスの感染経路検出方法とその方法に用いるトレースウィルスを記録する記録媒体を提供することにある。
【0009】
【課題を解決するための手段】請求項1の発明は、特定の情報処理領域内に外部から侵入し、マシン、プログラム、データファイル等の文書等へ自己複製し感染するコンピュータウィルスの感染ルートを追跡して検出するコンピュータウィルスの感染経路検出方法であって、コンピュータウィルスと同様の自己複製機能を有し、コンピュータウィルスと同様の感染経路をとると想定される感染履歴情報を記録するコンピュータウィルスと無関係のトレースウィルスを特定の調査領域内に蔓延させ、コンピュータウィルスが発見されたとき、発見された文書等に存在するトレースウィルスを起点にして特定の調査領域内のトレースウィルスの感染履歴情報を順次調べて、感染履歴情報に基づいてトレースウィルスの感染ルートを探索して特定し、特定されたトレースウィルスの感染ルートに基づいてコンピュータウィルスの感染ルートを推定して特定の調査領域への侵入箇所を検出するようにしたものである。この手段によれば、トレースウィルスの感染履歴を順次調べて、トレースウィルスの感染ルートに基づいてコンピュータウィルスの感染ルートを推定し、特定の調査領域へのコンピュータウィルスの侵入箇所が検出される。この結果、コンピュータウィルスが発見でき、駆除できても、感染経路の追跡ができないという従来の問題点が解決でき、感染の予防による感染の未然防止によって感染を根絶することができる。
【0010】請求項2の発明は、請求項1記載のコンピュータウィルスの感染経路検出方法において、文書等の感染元である親トレースウィルスと文書等の感染先である子トレースウィルスとの関係において、子トレースウィルスの感染履歴情報に親トレースウィルスの存する文書を特定する文書情報を記憶させ、コンピュータウィルスが発見されたとき、発見されたコンピュータウィルスに存在する文書のトレースウィルスの履歴情報によって親トレースウィルスの存する文書情報を順次特定してトレースウィルスの感染ルートを探索して特定しコンピュータウィルスの侵入箇所を検出するようにしたものである。この手段によれば、順次親トレースウィルスの文書情報に基づいて順次親文書に存在するコンピュータウィルスを確かめて、コンピュータウィルスの感染源である侵入箇所を検出するので、コンピュータウィルスの追跡が効率的にできる。
【0011】請求項3の発明は、請求項1記載のコンピュータウィルスの感染経路検出方法において、文書等の感染元である親トレースウィルスと文書等の感染先である子トレースウィルスとの関係において、親トレースウィルスの感染履歴情報に親トレースウィルスの存する文書を特定する子文書情報を記憶させ、コンピュータウィルスの侵入が検出されたとき、検出されたコンピュータウィルスに存在する文書のトレースウィルスの感染履歴

ように、トレースウィルス本体（１０１）の自己複製機能により、子のトレースウィルスを生む場合、親トレースウィルス１００の情報記録部（１０２）は、子トレースウィルス１００Ａの情報エリア（１０３）へ以下のように情報を記録する。

【００２７】すなわち、図３に示す情報エリア１０３の

（１）　２０１の日時部へは、子を生んだ日時を記録する。

（２）　２０２のマシンＩＤ部へは、子を生んだ時点での所在のマシンのＩＤ（例えばＩＰアドレスなど）を記録する。

（３）　２０３の文書ＩＤ部へは、（子のトレースウィルスが寄生（感染）している）宿主の文書名と、トレース感染が発生した時点で、宿主の文書が存在していたディレクトリパスを記録する。

（４）　２０４の親文書ＩＤ部へは、感染時点で、親のトレースウィルスから、上記２０３の文書ＩＤを引継ぎ、記録する。

【００２８】すなわち、トレースウィルス１００が親から子へと順次感染して行く過程では、図５に示すように、例えば、左側のトレースウィルス１００Ａから中央のトレースウィルス１００Ｂが感染して発生したとする。この場合、中央のトレースウィルス１００Ｂの情報エリア１０３には、左側のトレースウィルス１００Ａの１０２の情報記録機能によってトレースウィルス１００Ｂの固有の２０１（日時）Ｈ，１０，４，２６、２０２（マシンＩＤ）ＩＤ，Ａ００６、２０３（文書ＩＤ）ＩＤ，Ｂ００６が記録される。

【００２９】さらに、トレースウィルス１００Ｂの２０４（親子書）は、感染源であるトレースウィルス１００Ａの２０３（文書ＩＤ）ＩＤ，Ｂ００４がスライドして記録される（図示斜線矢印）。同様に、トレースウィルス１００Ｂが他の文書へ感染させトレースウィルス１００Ｃが発生したとき、トレースウィルス１００Ｃの情報エリア１０３の内で２０１～２０３は、トレースウィルス１００Ｃの個別値が記録され、２０４（親文書）には、親側に当たるトレースウィルス１００Ｂの２０３（文書ＩＤ）ＩＤ，Ｂ００６がスライドして記録される。これによって、下流（子側）から上流（親側）への追跡が可能となる。

【００３０】次に、本物のコンピュータウィルスが発見されたとき、トレースウィルス１００の記録を調べる（Ｓ３）。

【００３１】この場合、図６に示すように、親文書の感染経路の追跡がされる。まず、発見されたコンピュータウィルスの感染文書に同時に感染しているトレースウィルスの情報を取り出す（Ｓ１１）。続いて、トレースウィルス１００の情報エリア２０４の親文書ＩＤと一致する文書ＩＤ（２０３）を持つ文書を探し出す。その場合、２０２のマシンＩＤで示された同じマシン内の文書から着手することで、追跡は効率化できる。

【００３２】例えば、図５の例では、発見されたコンピュータウィルスの感染文書に同時にトレースウィルス１００Ｃがあった場合、トレースウィルス１００Ｃの情報エリア１０３の２０４（親文書ＩＤ）ＩＤ，Ｂ００６から同じ（文書ＩＤ）のトレースウィルス１００Ｂが親側と特定される。さらに、同様にトレースウィルス１００Ｂの２０４（親文書ＩＤ）から親側のトレースウィルス１００Ａが順次特定される。

【００３３】ただし、感染後、文書名が変更されたり、文書が移動されている場合も考えられる。この場合、文書名や、文書の存在するディレクトリパスとトレースウィルスの情報部とが一致しないため、他のディレクトリ、マシン内の“トレースウィルスの情報”の中から一致するものを探し出す必要がある。探し出された親文書が、発見されたコンピュータウィルスに感染しているか調べる（Ｓ１３）。この場合、コンピュータウィルスに感染していない親文書をみつけるか、社内（組織内）へのコンピュータウィルスの侵入点にたどりつくまで続ける（Ｓ１４）。

【００３４】次に、以上で辿られた経路から、逆に、図７に示すように、子文書の感染を追跡する。

【００３５】具体的には、起点となるトレースウィルスの情報エリア２０３の文書ＩＤと一致する親文書ＩＤ（２０４）を持った文書を探し出す（Ｓ２１）。

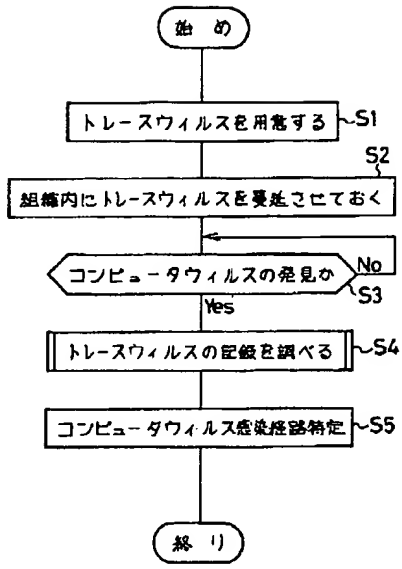
【００３６】例えば、図５の例によれば、起点となるトレースウィルス１００として左側のトレースウィルス１００Ａが特定された場合、情報エリア１０３の２０３（文書ＩＤ）ＩＤ，Ｂ００４と同じＩＤ，Ｂ００４を情報エリア１０３の２０４（親文書）を有するトレースウィルス１００を探し出す。例えば、中央のトレースウィルス１００Ｂであるが複数存在することが考えられる。

【００３７】ただし、感染後、文書名が変更されたり、文書が移動されている場合も考えられる。この場合、文書名や、文書の存在するディレクトリーパスとトレースウィルスの情報部とが一致しないため、他のディレクトリー、マシン内の“トレースウィルスの情報”の中から一致するものを探し出す必要がある。

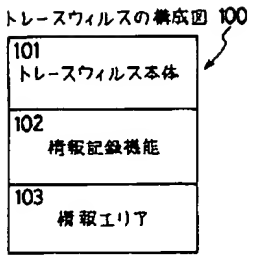
【００３８】また、親のトレースウィルスの日時情報（２０１）以降の作成・変更日時を持つ文書を絞り込むことにより、探索を効率化することもできる。さらに、探し出された子文書が、発見されたウィルスに感染しているか調べる（Ｓ２２）。Ｓ２１，Ｓ２２を図６の処理Ｓ１１～Ｓ１５で発見された感染経路から派生するすべての経路に対してウィルスに感染していない文書をみつけるまで続ける（Ｓ２３）。

【００３９】図８に示す簡単な例では、文書Ｊ（図示太線矢印）で本物のコンピュータウィルスが発見されたと仮定し、図６に示す手順で、トレースウィルス１００の情報エリア１０３の親文書ＩＤと一致する文書ＩＤを持

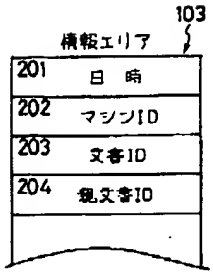
【図1】



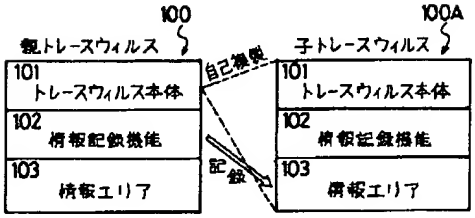
【図2】



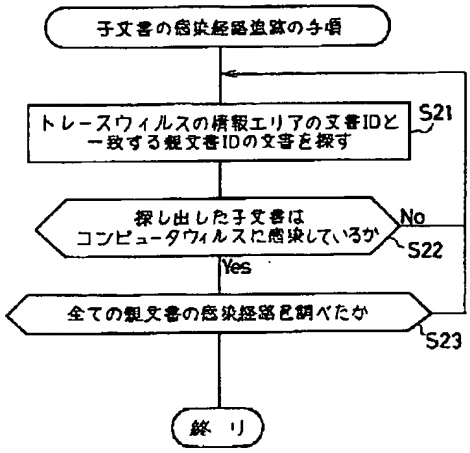
【図3】



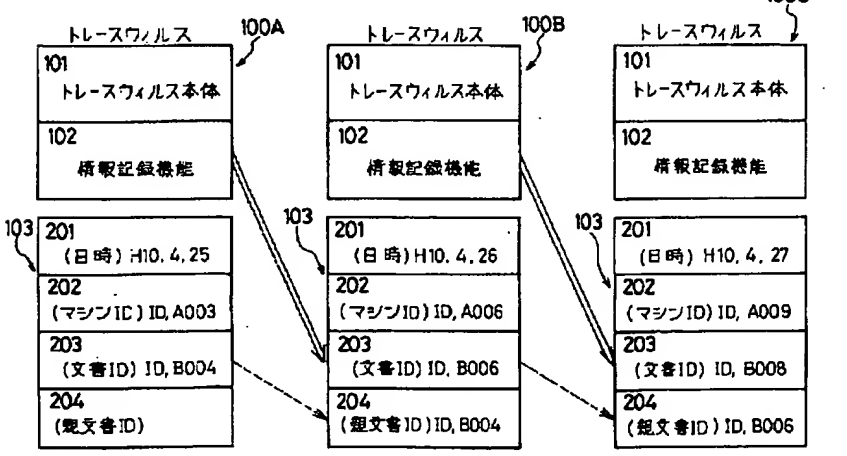
【図4】



【図7】



【図5】



【図9】